DISEÑO DEL SOFTWARE PARA EL SEGUIMIENTO Y CONTROL DE FRAUDES TRANSACCIONALES DESDE INTERNET Y BANCA MOVIL CON TARJETA DEBITO BAJO LOS LINEAMIENTOS DEL PMI

AUTOR

STEFFANY D. CATALINA ANGARITA BECERRA
Ingeniera Industrial
k_tik90@hotmail.com
Steffany.kata@gmail.com

Artículo Trabajo Final del programa de Especialización en Gerencia Integral de Proyectos

DIRECTOR

Ing. Freddy León Reyes, M.Ed.

Ingeniero de sistemas con énfasis en software - Universidad Antonio Nariño
Especialista en Docencia Universitaria de la Universidad Nueva Granada
Magíster en educación de la Universidad Nueva Granada
Director Académico Programa Ingeniería en Multimedia de la Universidad Militar Nueva Granada
freddy.leon@unimilitar.edu.co

ESPECIALIZACIÓN EN GERENCIA INTEGRAL DE PROYECTOS
UNIVERSIDAD MILITAR NUEVA GRANADA
FACULTAD DE INGENIERÍA
DICIEMBRE 2016

DISEÑO DEL SOFTWARE PARA EL SEGUIMIENTO Y CONTROL DE FRAUDES TRANSACCIONALES DESDE INTERNET Y BANCA MOVIL CON TARJETA DEBITO BAJO LOS LINEAMIENTOS DEL PMI

DESIGN OF THE SOFTWARE FOR MONITORING AND CONTROL TRANSACTIONAL FRAUDS FROM THE INTERNET AND MOBILE BANKING WITH DEBIT CARD UNDER THE GUIDELINES OF THE PMI

STEFFANY D. CATALINA ANGARITA BECERRA
Ingeniera Industrial
k_tik90@hotmail.com
steffany.kata@gmail.com

RESUMEN

El presente artículo expone los principales lineamientos del PMI para el seguimiento y control de fraudes transaccionales desde internet y banca móvil con tarjeta débito, el cual establece de manera precisa, adecuada y eficiente el desarrollo para el diseño del sistema de monitoreo.

A través de la ejecución de este documento, es posible obtener una pauta que permite a las entidades financieras, exponer procesos más seguros implementando la metodología expuesta, presentando las causas y los beneficios de obtener un control y seguimiento en las transacciones con tarjeta debito desde los portales de internet y banca móvil.

Palabras Clave: PMI, Seguimiento y control, Entidades financieras, Aplicaciones web, Internet, Banca Móvil.

ABSTRACT

This article presents the main guidelines of the PMI for monitoring and controlling in frauds transactional on Internet and mobile banking using debit card, which establishes in precise way and efficient way the development for the design of monitoring system.

Through the execution of this document, it is possible to obtain a guideline what allows financial institutions to expose the most secure processes implementing the presented methodology, present the causes and benefits of obtaining a monitoring and control on transactions using debit cards in web portals on internet and mobile banking.

Keywords: PMI, Monitoring and controlling, financial entities, web applications, Internet, Mobile Banking.

INTRODUCCIÓN (3 páginas)

La innovación financiera de la mano de la tecnología representa hoy uno de los elementos esenciales, por lo cual, se facilita el acceso a los servicios financieros y se disminuyen costos asociados a los mismos.

Se analizó diferentes aspectos de demanda realizada este año por la Superintendencia Financiera, en donde se encontró que el último año se realizaron 3,717 millones de transacciones equivalentes por un monto total de $6,359 billones, destacándose el crecimiento en el uso de canales transaccionales no presenciales como internet y banca móvil. [1]

- El canal más representativo corresponde al internet (37%).
- La banca móvil registró a 2014 un aumento del 54%, en donde se resalta la participación de las operaciones no monetarias como la consulta de saldo un (83%) [1].

La Superfinanciera reconociendo los riesgos inherentes en los canales, obligó a las entidades destinatarias al cumplimiento de un elemento imperativo; la autenticación del usuario en el respectivo canal, previo, a la realización de la operación. En el caso del canal Internet, la circular obligó al uso de mecanismos fuertes de autenticación como la biometría, certificados de firmas digitales, one time password o claves de un solo uso, entre otros [1].

De otra parte, para banca móvil, la normativa no exigió mecanismos fuertes de autenticación, solo mecanismos de autenticación de dos factores, pero reitera, que en caso de hacer uso del dispositivo móvil para ingresar al banco por el navegador, será catalogado como banca por Internet, es decir requiere un mecanismo fuerte de autenticación [1].

La realización de una determinada operación vía celular o internet deberá estar precedida del cumplimiento de los procedimientos establecidos por cada establecimientos comerciales, así como de los protocolos de seguridad previamente señalados y que en el caso de transferencia de dineros, cuando menos deberá estar precedida de la preinscripción de la cuenta o cuentas receptoras junto con los demás mecanismos de validación y autenticación del cliente. Sin embargo, la barrera determinante para el resto de personas que no realicen transacciones a través de estos canales se debe a la inseguridad de los sistemas para realizar movimientos financieras por celular e internet. Con frecuencia, estas inseguridades se deben por realizar actos de comercio de forma inadecuada corriendo el riesgo de que su información sea sustraída por terceros [1].

Es así como, es necesario implementar un monitoreo en línea de transacciones con tarjeta debito que constituya una herramienta importante para las entidades financieras, que quieren minimizar los riesgos de pérdida de capital. Este diseño del sistema de monitoreo atraerá los siguientes beneficios los cuales se describen a continuación: Manejo con exactitud de las transacciones desde internet y banca móvil, mejoramiento de la seguridad enfocado exclusivamente en protección contra fraude electrónico, disminución de calificación de transacciones basadas en riesgos y ofreceremos soluciones multi-canal para combatir Phishing [1].

También obtendremos contra beneficios como son: El sistema de monitoreo solo se enfocará a las transacciones realizadas con tarjeta debito en los canales electrónicos (Internet y banca móvil) y su implementación solo se tiene contemplado para entidades financieras.

El proyecto es factible porque cuenta con un estudio de mercado, técnico y financiero, donde aportará la disminución de errores, mayor precisión e integración de todas las áreas, reducción de tiempo de respuesta a quejas y reclamos, mejoramiento en los servicios transacciones desde internet y banca móvil a los clientes.

El proyecto incurriría en los siguientes costos directos e indirectos de operación: Mano de obra directa e indirecta, infraestructura tecnológica (hardware), software, creación de ambientes (desarrollo, prueba y producción), plan de capacitación, Gastos de administración y venta. El Proyecto es viable porque sus costo son alcanzables, y en el cual el sistemas de monitoreo permitirá seguimiento y control en las transacciones electrónicas de manera automatizada en tiempo real realizadas con las tarjetas débito, con el objetivo de detectar y prevenir los fraudes electrónicos realizados desde internet y banca móvil.

1. MATERIALES Y MÉTODOS

1.1 Transacciones que se pueden realizar desde internet y banca móvil con tarjeta débito.

En la actualidad, las entidades bancarias le ofrecen diversos canales tecnológicos a través de los cuales puede realizar transacciones financieras y al mismo tiempo, ahorrar tiempo y dinero en desplazamientos, por ejemplo:

La banca móvil es un servicio proporcionado por entidades financieras que permite a sus clientes realizar una serie de transacciones monetarias de forma remota mediante un dispositivo móvil como un teléfono móvil o tablet, y el uso de software, que generalmente se llama aplicación, proporcionadas por la institución financiera para tal propósito. La banca móvil está normalmente disponible las 24 horas. Algunas instituciones financieras tienen restricciones en algunas cuentas al acceder a través de la banca móvil, así como un límite en la cantidad que puede ser tranzado [1].

Los tipos de transacciones financieras que un cliente puede realizar a través de banca móvil incluyen la obtención de saldos de la cuenta y la lista de transacciones más recientes, pagos de factura electrónica y transferencias de fondos entre cuentas de un cliente o a otro [1].

Portal Internet, banca por Internet o en línea comprende aquellas herramientas que ofrecen una entidad para que sus clientes hagan sus operaciones bancarias a través de la computadora utilizando una conexión a la red Internet [1].

Los tipos de transacciones financieras que un cliente puede realizar a través de internet son:

1.1.1 Consultas:

1.1.1.1 Resumen de productos.
1.1.1.2 Movimiento de productos.
1.1.1.3 Consulta de extractos: Cuentas, Tarjeta de crédito y créditos.
1.1.1.4 Consulta de certificados.

1.1.2 Las transacciones monetarias:

1.1.2.1 Pago de tarjeta crédito Propia, AVAL y ACH.
1.1.2.2 Transferencia de cuentas al mismo Banco, AVAL, ACH.
1.1.2.3 Pagos de servicios Público, Impuestos y PILA.
1.1.2.4 Pago de Créditos propios, AVAL, ACH.
1.1.2.5 Donaciones.
1.1.2.6 Pagos de impuesto Distritales.
1.1.2.7 Pago de PILA.
1.1.2.8 Avance de tarjeta crédito con abono a cuenta.
1.1.2.9 Utilización de créditos rotativos con abono a cuenta asociadas.

1.1.3 Servicios:

1.1.3.1 Crear alertas y notificaciones
1.1.3.2 Actualizar datos
1.1.3.3 Bloquear tarjeta debito
1.1.3.4 Cambio de clave de tarjetas débitos.
1.1.3.5 Cambiar parámetros de topes y montos para Canales Electrónicos.

1.2 Identificación de causas de fraudes transaccionales desde internet y banca móvil con tarjeta debito

Los delincuentes ahora utilizan diferentes técnicas informáticas para atacar a los usuarios de los bancos. Lo que buscan es obtener los datos de las personas, ya sea información personal, de sus productos financieros (qué tarjetas de crédito tiene asociadas) o información de seguridad de sus cuentas (usuario y contraseñas de acceso). Las técnicas más utilizadas son *el phishing, el smishing y el malware*. [2]

En el *phishing,* los delincuentes suplantan la página Web de la entidad, envían correos electrónicos o genera una ventana emergente invitando al cliente a ingresar a la página e ingresar sus datos financieros o la autenticación de la cuenta. Sobre la página fraudulenta, el delincuente captura la información del cliente y la almacena para su uso fraudulento que puede utilizar directamente o vender a otros delincuentes, señala Daniel Castellanos, vicepresidente económico de Asobancaria. [2]

El *smishing* es una práctica en la que los delincuentes hacen uso de los mensajes de texto de los celulares y la ingeniería social para engañar a las personas y obtener información financiera o información útil para el robo de identidad, sostiene castellano. Los delincuentes generalmente ofrecen premios. [2]

Por su parte, el software espía (*malware*), es una modalidad en la que los delincuentes monitorean las actividades del usuario del computador, como las páginas que visita o el tipo de información busca, e incluso la información que escribe en el teclado y los contenidos de sus correos electrónicos [2].

Lo más grave es que cuando el usuario utiliza su computador para acceder a Internet y hacer sus transacciones bancarias, el software va capturando y enviando la información al delincuente sin que el cliente se dé cuenta [2].

La instalación del software espía se puede realizar a través de un hardware (como USB o CD) o se instala automáticamente, sin que el usuario se dé cuenta, cuándo baja programas de sitios no seguros o abre correos electrónicos que no sabe de donde provienen [2].

Una vez con los datos del cliente, el delincuente puede realizar las siguientes transacciones electrónicas: transferencias a cuentas del mismo banco, transferencias

a cuentas de otro banco, pagos a terceros (servicios públicos, celulares, etc.), compras o pagos por Internet a través de PSE o compras con tarjeta de crédito por Internet o banca móvil [2].

Sin embargo, Un alto porcentaje de fraude cuenta con la participación de empleados de las empresas en donde ocurre el hecho [2].

Actitud reactiva frente al fraude: La actitud de la gerencia frente al fraude suele ser reactiva. Más de la mitad de los fraudes en las empresas son descubiertos por coincidencia, ya sea por información obtenida por medios externos, accidentes o cambios en la administración, entre otros factores [2].

Falta de conocimiento del negocio: Por lo general, las directivas tienen un conocimiento <menos que bueno> de las operaciones en los negocios principales y, en menor grado, de sus operaciones en otros países [2].

Los directivos tienden a delegar la responsabilidad de implementar controles para prevenir grandes fraudes. La mayoría piensa que los auditores deben poder detectar los fraudes substanciales como parte de sus auditorías normales, a la vez que no están dispuestos a pagar más por pasarles la responsabilidad a sus auditores [2].

Lo anterior sugiere que la gerencia debe asumir plenamente la responsabilidad o admitir que en el momento se le está delegando a la gente equivocada, pensando que los controles no siempre sirven [2].

Se piensa que los altos directivos pueden sobrepasar los controles. Un alto directivo o gerente que busque realizar un gran fraude puede sobrepasar los controles internos establecidos [2].

Mínima parte de las empresas que han tenido casos de fraude los han denunciado. En lo que respecta a las empresas que no denunciaron los fraudes, los costos, el temor a que el caso afectara su Ilustración y la incertidumbre con respecto a los resultados son las principales razones para no hacerlo [2].

La acción de las autoridades frente al fraude: La gran mayoría, considera que las cortes (el sistema judicial) no entienden la complejidad de los principales casos de fraude y, por lo tanto, no fallan de manera satisfactoria [2].

1.3 Características reglamentarias para el seguimiento y control de las transacciones en internet y banca móvil

Para el cumplimiento de los requerimientos mínimos de seguridad y calidad de la información que se maneja a través de canales e instrumentos para la realización de operaciones, las entidades deberán tener en cuenta las siguientes definiciones y criterios [3]:

1.3.1 Criterios de seguridad de la información:

1.3.1.1 Confidencialidad: Hace referencia a la protección de información cuya divulgación no está autorizada [3].
1.3.1.2 Integridad: La información debe ser precisa, coherente y completa desde su creación hasta su destrucción [3].
1.3.1.3 Disponibilidad: La información debe estar en el momento y en el formato que se requiera ahora y en el futuro, al igual que los recursos necesarios para su uso [3].

1.3.2 Criterios de calidad de la información:

1.3.2.1 Efectividad: La información relevante debe ser pertinente y su entrega oportuna, correcta y consistente. [3]
1.3.2.2 Eficiencia: El procesamiento y suministro de información debe hacerse utilizando de la mejor manera posible los recursos. [3]
1.3.2.3 Confiabilidad: La información debe ser la apropiada para la administración de la entidad y el cumplimiento de sus obligaciones. [3]

1.3.3 Internet

Las entidades que ofrezcan la realización de operaciones por Internet deberán cumplir con los siguientes requerimientos [4]:

1.3.1.1 Implementar los algoritmos y protocolos necesarios para brindar una comunicación segura [4].
1.3.1.2 Realizar como mínimo dos veces al año una prueba de vulnerabilidad y penetración a los equipos, dispositivos y medios de comunicación usados en la realización de operaciones monetarias por este canal. Sin embargo, cuando se realicen cambios en la plataforma que afecten la seguridad del canal, deberá realizarse una prueba adicional [4].
1.3.1.3 Promover y poner a disposición de sus clientes mecanismos que reduzcan la posibilidad de que la información de sus operaciones monetarias pueda ser capturada por terceros no autorizados durante cada sesión. [4]
1.3.1.4 Establecer el tiempo máximo de inactividad, después del cual se deberá dar por cancelada la sesión, exigiendo un nuevo proceso de autenticación para realizar otras operaciones [4].
1.3.1.5 Informar al cliente, al inicio de cada sesión, la fecha y hora del último ingreso a este canal [4].
1.3.1.4 Implementar mecanismos que permitan a la entidad financiera verificar constantemente que no sean modificados los enlaces (links) de su sitio Web, ni suplantados sus certificados digitales, ni modificada indebidamente la resolución de sus DNS [4].
1.3.1.5 Contar con mecanismos para incrementar la seguridad de los portales, protegiéndolos de ataques de negación de servicio, inyección de código malicioso u objetos maliciosos, que afecten la seguridad de la operación o su conclusión exitosa [4].

1.3.1.6 Las entidades que permitan realizar operaciones monetarias por este anal deben ofrecer a sus clientes mecanismos fuertes de autenticación [4].

1.3.2 Banca Móvil

El canal de Banca Móvil deberá cumplir con los siguientes requerimientos [5]:

1.3.2.1 Contar con mecanismos de autenticación de 2 factores para la realización de operaciones monetarias y no monetarias [5].

1.3.2.2 Para operaciones monetarias individuales o que acumuladas mensualmente por cliente superen 2 SMMLV, implementar mecanismos de cifrado fuerte de extremo a extremo para el envío y recepción de información confidencial de las operaciones realizadas, tal como: clave, número de cuenta, número de tarjeta, etc., [5].

1.3.2.3 Cualquier comunicación que se envíe al teléfono móvil como parte del servicio de alertas o notificación de operaciones no requiere ser cifrada, salvo que incluya información confidencial [5].

1.3.2.4 Para las operaciones monetarias individuales o que acumuladas mensualmente por cliente sean inferiores a 2 SMMLV y que no cifren la información de extremo a extremo, la entidad deberá adoptar las medidas necesarias para mitigar el riesgo asociado a esta forma de operar, el cual debe considerar los mecanismos de seguridad en donde la información no se encuentre cifrada. La Superintendencia Financiera de Colombia (SFC) podrá suspender el uso del canal cuando se advierta que existen fallas que afecten la seguridad de la información [5].

1.3.2.5 Contar con medidas que garanticen la atomicidad de las operaciones y eviten su duplicidad debido a fallas en la comunicación ocasionadas por la calidad de la señal, el traslado entre celdas [5].

2 RESULTADOS Y DISCUSIONES

2.1 Diseñar el plan de control y seguimiento según metodología PMI.

El seguimiento y control de las transacciones con tarjeta debito desde internet y banca móvil, se desarrolla dentro del marco de la metodología PMI, está constituido por 5 etapas que son: Inicio, planeación, ejecución, seguimiento y control, y cierre. Dentro de la fase de ejecución se tiene contemplado el desarrollo del producto, la migración de datos y la capacitación funcional y técnica. El desarrollo del producto se hará en siete ciclos; cada uno de los ciclos contiene las 4 fases de la metodología RUP que son: Concepción, elaboración, construcción y transición. El software a su vez se hará en 4 iteraciones y cada una de ellas contiene las siguientes 7 etapas: Planeación, diseño, desarrollo, pruebas, documentación, implementación y mantenimiento, para finalmente ejecutar el proceso definitivo del software y de esta manera tener el 100% del sistema disponible para iniciar el proceso de implantación.

Como se evidencia en la Ilustración 1, el proceso de desarrollo es iterativo e incremental, se utilizará un modelo de V el cual propone las etapas de análisis, diseño, implementación, pruebas y a su vez planeación de pruebas funcionales, de sistema, de integración y unitarias, de modo que al momento de llegar a la etapa de pruebas se ejecute en orden inverso las pruebas planeadas finalizando con las de usuario.

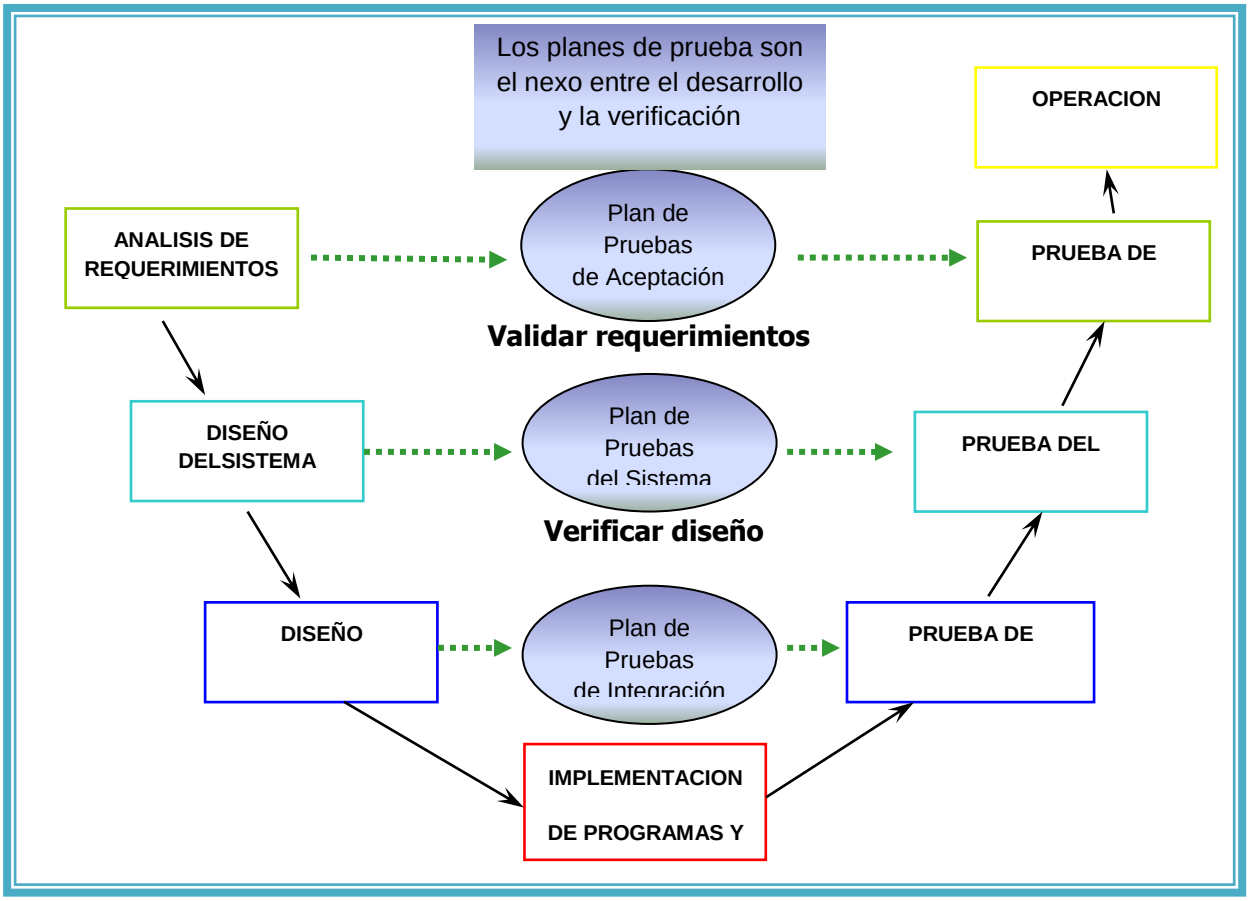

Ilustración 1. Modelo en V

Fuente. Ministerio de Defensa de Alemania, 1992

2.2. Gestionar las actividades del seguimiento y control de las transacciones con tarjeta debito desde internet y banca móvil.

Para especificar las actividades es necesario definir la estructura de desglose del trabajo (EDT) y el detalle de cada fase del proyecto con sus respectivas actividades, en los apartados 2.2.1 y 2.2.2 que se encuentran a continuación se detallara cada paso para la gestión de actividades.

2.2.1 Obtener la estructura de desglose de trabajo EDT.

La estructura de desglose del trabajo EDT, es unas estructuras exhaustivas, jerárquicas y descendentes formadas por las entregables necesarias para el proyecto, para el sistema de control y seguimientos construyo la EDT donde se inició con el Objetivo del proyecto, desagregación de las fases, y por ultimo identificación de las actividades. En la Ilustración 2, se ilustra la estructura de trabajo del diseño del software para el seguimiento y control de fraudes transaccionales desde internet y Banca móvil con tarjeta debito bajo los lineamientos del PMI.

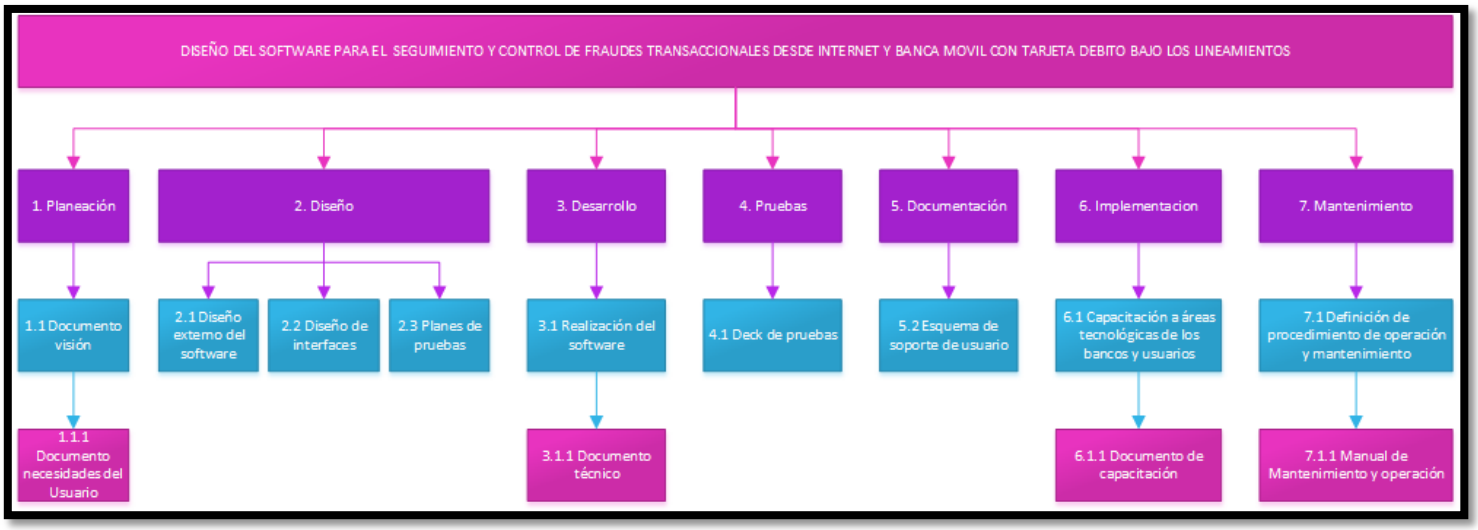

Ilustración 2: Estructura de desglose de trabajo (EDT).

La EDT del proyecto se divide en siete fases (Planeación, diseño, ejecución, pruebas, documentación, implementación y mantenimiento) y en cada fase se tienen varios paquetes de trabajo.

En la etapa de planeación se incluyen las actividades de elaboración del Project chárter, la identificación de todas las personas u organizaciones que puedan ser afectados positiva o negativamente, por la ejecución del proyecto. El Project chárter es el documento que se presentara a los clientes para obtener la aprobación de inicio del proyecto, y contiene los aspectos fundamentales del proyecto.

En el paquete de trabajo de análisis se realiza un levantamiento de información sobre la locación donde se implementará el sistema de control de fraudes y se hace un pre diseño de software.

En la segunda etapa, diseño, se realiza el diseño detallado de software, sistemas de comunicación y el software.

En la etapa de ejecución, se realiza la adquisición de dispositivos y partes eléctricas, su posterior instalación, y paralelamente se desarrollaría el software.

En la cuarta etapa, pruebas, se realizan pruebas al sistema completo y en caso de encontrar algún error se corrigen. En la etapa final se elabora la documentación concerniente al proyecto (software y manual).

2.3 Detalle de cada fase y etapa del diseño del software para seguimiento y control de fraudes transaccionales.

Se describe las actividades del seguimiento y control para evitar fraudes transaccionales desde internet y banca móvil donde se evidencia que consta de 7 fases y cada fase cuenta con actividades, las cuales son:

2.3.1. Fase Planeación: En esta fase se analizan los procesos requeridos para establecer el alcance del proyecto, definir los objetivos y el curso de acción necesaria para alcanzarlos en los tiempos y costos establecidos.

En esta fase se establece el análisis de requisitos a desarrollar, siendo necesario especificar los procesos y diagrama de flujo de datos que se van a emplear.

En el análisis estructurado se incluirá:

2.3.1.1. Diagramas de flujo de datos: Sirven para conocer el comportamiento del sistema mediante representaciones gráficas.
2.3.1.2. Modelos de datos: Sirven para conocer las estructuras de datos y sus características (Entidad relación y formas normales).
2.3.1.3. Diccionario de datos: Sirven para describir todos los objetos utilizados en los gráficos, así como las estructuras de datos.
2.3.1.4. Definición de los interfaces de usuario: Sirven para determinar la información de entrada y salida de datos.

2.3.2. Fase de Diseño: En esta etapa del proyecto se hará todo el análisis, diseño y del software para mitigar los fraudes transacciones desde internet y Banca móvil con tarjeta débito. En el diseño estructurado se define:

2.3.2.1 Diseño externo: Se especifican los formatos de información de entrada salida. (Pantalla y listados)
2.3.2.2 Diseño de datos: Establece las estructuras de datos de acuerdo con su soporte físico y lógico. (Estructuras en memoria, ficheros y hojas de datos)
2.3.2.3 Diseño modular: Es una técnica de representación en la que se refleja de forma descendente la división de la aplicación en módulos. Está basado en diagramas de flujo de datos obtenidos en el análisis.

2.3.2.4 Diseño procedimental: Establece las especificaciones para cada módulo, escribiendo el algoritmo necesario que permita posteriormente una rápida codificación.

2.3.3. Fase Desarrollo: En esta fase se alcanza con mayor precisión una solución óptima de la aplicación, teniendo en cuenta los recursos físicos del sistema (tipo de ordenador, periféricos, comunicaciones) y los recursos lógicos. (Sistema operativo., programas de utilidad, bases de datos), se realiza el desarrollo y pruebas técnicas del software.

2.3.4. Fase pruebas: En esta fase se analiza documento funcional y documento de desarrollo, se efectúa documento de casos de pruebas y realización de las siguientes pruebas:

2.3.4.1 Pruebas de Compatibilidad: Son las pruebas que se realizarán en un software o aplicación determinado y que comprobarán que tu desarrollo es compatible con todos los navegadores de Internet y todos los sistemas convenientes. Estas pruebas son realmente importantes para que tu producto llegue a todos los usuarios que deberían de llegar y que todo el mundo pueda utilizarlo con lo que disponga en su equipo informático.

2.3.4.2 Pruebas de regresión: Se evalúa el correcto funcionamiento del software desarrollado frente a evoluciones o cambios funcionales. El propósito de éstas es asegurar que los casos de prueba que ya habían sido probados y fueron exitosos permanezcan así. Se recomienda que este tipo de pruebas sean automatizadas para reducir el tiempo y esfuerzo en su ejecución.

2.3.4.3 Pruebas de Integración: Es el nivel de pruebas posterior a las pruebas modulares de los componentes de un sistema. Se centra principalmente en probar la comunicación entre los componentes de un mismo sistema, comunicación entre sistemas o entre hardware y software.

2.3.5. Fase Documentación: En esta etapa se tendrá en cuenta las siguientes actividades: Preparación y documentación del software, realización de capacitaciones, evaluación de entendimiento de capacitaciones, realizar de manuales de operaciones y mantenimiento del software, realización del proceso de los canales internet y banca móvil.

2.3.6. Fase de implementación: Es esta fase es la puesta en producción, en la etapa de Implementación comenzamos con el resultado de la etapa de Diseño e implementamos el sistema en términos de componentes, es decir, ficheros de código fuente, scripts, ficheros de código binario, ejecutables y similares.

2.3.7. Fase de Mantenimiento: En esta fase se debe generar y actualizar el denominado documento de historia del proyecto (DHP); documento que incluye todos los errores (y sus correcciones) y/o modificaciones realizadas del software.

En la tabla 1. Actividades del proyecto, se detalla las fases y actividades que se realizara para seguimiento y control de fraudes transaccionales desde internet y banca móvil**.**

Tabla 1. Actividades del proyecto.

PROYECTO BANCA MOVIL E INTERNET
1. PLANEACION
1.1 Aprobar del alcance
1.2 Definir y aprobar de objetivos
1.3 Aprobar de materiales
1.4 Analizar de requisitos
1.5 Documentar formal de los requisitos
1.6 Analizar estructural
1.6.1 Diseñar diagrama de flujo de datos
1.6.2 Realizar el modelo de datos
1.6.3 Ejecutar el diccionario de datos
2. DISEÑO
2.1Análizar el desarrollo, tiempos de diseño de la aplicación
2.2 Realizar diseño externo del software
2.3 Realizar diseño de datos
2.4 Realizar diseño modular
2.5 Realizar diseño procedimental
3. DESARROLLO
3.1 Desarrollar Software
3.2 Ejecutar pruebas técnicas
3.3 Entregar documento final del desarrollo
4. PRUEBAS
4.1 Verificar documento funcional final del desarrollo
4.1.1 Realizar documento de casos de pruebas
4.2 Ejecutar Pruebas de compatibilidad
4.3 Ejecutar Pruebas de regresión
4.4 Ejecutar Pruebas de integración
5. DOCUMENTACION
5.1 Preparar y documentar la capacitación del software
5.2 Realizar las capacitaciones
5.3 Diligenciar registro de capacitaciones
5.4 Realizar manuales de operación y mantenimiento de software
5.5 Documentar el proceso del canal Banca móvil
6. IMPLEMENTACION
6.1 Realizar la puesta en producción
7. MANTENIMIENTO
7.1 Realizar documento de historia del proyecto. (DHP

2.4 Gestionar el tiempo de realización para el seguimiento y control de las transacciones con tarjeta debito desde internet y banca móvil.

Para especificar los tiempos es necesario definir el detalle de cada fase del proyecto con sus respectivas actividades valorando tiempo de inicio y finalización, definir los

recursos y la asignación de participación de cada uno de ellos, establecer el diagrama de precedencia y por ultimo obtener la ruta crítica, en los apartados 2.3.1, 2.3.2, 2.3.3 y 2.3.4 que se encuentran a continuación se detallara cada paso para la gestión de tiempo.

2.4.1 Cronograma detallado

Durante la fase de Planeación se trabajó en la elaboración del cronograma del proyecto, para lo cual se tuvo en consideración los siguientes elementos:

2.4.1.1 La WBS
2.4.1.2 El modelo de procesos de negocio.
2.4.1.3 El inventario de casos de uso.
2.4.1.4 La estrategia de iteraciones en la construcción del software.
2.4.1.5 El plan de capacitación funcional.
2.4.1.6 La estrategia de Puesta en Marcha del software.

Todas las actividades de ingeniería de software, tanto del desarrollo como de la construcción y ejecución del monitoreo, se ejecutarán antes del 01 de octubre de 2017 con el fin de disponer de tiempo para las actividades de transición, capacitación y puesta en marcha de la solución.

Como se ilustra en la tabla 2. Cronograma de actividades, se estableció los elementos, particularmente con la WBS se estructuró la descomposición de actividades principales y sub-actividades y se preparó el cronograma general del proyecto, al cual se le establecieron precedencias entre las tareas tomando en consideración los siguientes criterios:

Tabla 2. Cronograma de actividades.

No.	ACTIVIDADES	Duración DIAS	Porcentaje	Comienzo	Fin
1	**PROYECTO BANCA MOVIL E INTERNET**	**360**	**100%**		
2	**1. PLANEACION**	**105**	**29%**		
3	1.1 Aprobar del alcance	15	**4%**	1/10/2016	16/10/2016
4	1.2 Definir y aprobar de objetivos	15	**4%**	17/10/2016	1/11/2016
5	1.3 Aprobar de materiales	7	**2%**	2/11/2016	9/11/2016
6	1.4 Analizar de requisitos	10	**3%**	10/11/2016	20/11/2016
7	1.5 Documentar formal de los requisitos	10	**3%**	21/11/2016	1/12/2016
8	1.6 Analizar estructural	15	**4%**	2/12/2016	17/12/2016
9	1.6.1 Diseñar diagrama de flujo de datos	15	**4%**	18/12/2016	2/01/2017
10	1.6.2 Realizar el modelo de datos	9	**3%**	3/01/2017	12/01/2017
11	1.6.3 Ejecutar el diccionario de datos	9	**3%**	13/01/2017	22/01/2017

12	**2. DISEÑO**	**41**	**11%**		
13	2.1Análizar el desarrollo, tiempos de diseño de la aplicación	10	**3%**	23/01/2017	2/02/2017
14	2.2 Realizar diseño externo del software	10	**3%**	3/02/2017	13/02/2017
15	2.3 Realizar diseño de datos	7	**2%**	14/02/2017	21/02/2017
16	2.4 Realizar diseño modular	7	**2%**	22/02/2017	1/03/2017
17	2.5 Realizar diseño procedimental	7	**2%**	2/03/2017	9/03/2017
18	**3. DESARROLLO**	**63**	**18%**		
19	3.1 Desarrollar Software	40	**11%**	10/03/2017	19/04/2017
20	3.2 Ejecutar pruebas tecnicas	15	**4%**	20/04/2017	5/05/2017
21	3.3 Entregar documento final del desarrollo	8	**2%**	6/05/2017	14/05/2017
22	**4. PRUEBAS**	**90**	**25%**		
23	4.1 Verificar documento funcional final del desarrollo	30	**8%**	15/05/2017	14/06/2017
24	4.1.1 Realizar documento de casos de pruebas	10	**3%**	15/06/2017	25/06/2017
25	4.2 Ejecutar Pruebas de compatibilidad	20	**6%**	26/06/2017	16/07/2017
26	4.3 Ejecutar Pruebas de regresión	10	**3%**	17/07/2017	27/07/2017
27	4.4 Ejecutar Pruebas de integración	20	**6%**	28/07/2017	17/08/2017
28	**5. DOCUMENTACION**	**43**	**12%**		
29	5.1 Preparar y documentar la capacitación del software	8	**2%**	18/08/2017	26/08/2017
30	5.2 Realizar las capacitaciones	5	**1%**	27/08/2017	1/09/2017
31	5.3 Diligenciar registro de capacitaciones	5	**1%**	2/09/2017	7/09/2017
32	5.4 Realizar manuales de operación y mantenimiento de software	15	**4%**	8/09/2017	23/09/2017
33	5.5 Documentar el proceso del canal Banca móvil	10	**3%**	24/09/2017	4/10/2017
34	**6. IMPLEMENTACION**	**10**	**3%**		
35	6.1 Realizar la puesta en producción	10	**3%**	5/10/2017	15/10/2017

36	**7. MANTENIMIENTO**	**8**	**2%**		
37	7.1 Realizar documento de historia del proyecto. (DHP)	8	**2%**	16/10/2017	24/10/2017

2.4.2 Recursos

El proyecto requiere de 7 personas profesionales dedicadas el 100%, los perfiles solicitados son: Ingeniero de sistemas, con especialización de Gerencia Integral de proyectos con 2 años de experiencia en proyecto para el cargo de Gerente del proyecto, Un ingeniero de sistemas con 5 años de experiencia para el cargo de Líder técnico, un ingeniero industrial con 3 años en documentación para Asesor Funcional, una ingeniera de sistemas con un año de experiencia en pruebas de software para el cargo de Líder de pruebas, un diseñador gráfico con un año de experiencia en diseños web para el cargo de Diseñador gráfico, un Ingeniero de sistemas con 3 años de experiencia desarrollando para el cargo de Desarrollador Senior.

Tabla 3. Recursos

CARGO	*DEDICACION*
1. Gerente de Proyecto	100% en todas las fases del proyecto
2. Líder Técnico	83% en todas las fases del proyecto
3. Asesor funcional	67% en las fases inicio, planeación y ejecución hasta la actividad de modelamiento de negocio.
4. Líder de Pruebas	25% en todas las fases del proyecto
5. Diseñador Grafico	17% en la fase de ejecución dentro de las actividades de diseño grafico
6. Arquitecto de Software	83% en todas las fases del proyecto
7. Desarrollador Senior	83% en todas las fases del proyecto

2.4.3 Obtener el diagrama de precedencias

Para obtener el diagrama de precedencia se utilizó la herramienta de actividades antecesoras y predecesoras.

Tabla 4. Actividades predecesoras

No.	ACTIVIDADES	PREDECESORAS	Duración DIAS	inicio	final
A	1.1 Aprobar del alcance		15	0	15
B	1.2 Definir y aprobar de objetivos	A	15	15	30
C	1.3 Aprobar de materiales	B	7	30	37
D	1.4 Analizar de requisitos	C	10	37	47
E	1.5 Documentar formal de los requisitos	D	10	37	47
F	1.6 Analizar estructural	D,E	15	47	62

G	1.6.1 Diseñar diagrama de flujo de datos	F	15	62	77
H	1.6.2 Realizar el modelo de datos	G	9	77	86
I	1.6.3 Ejecutar el diccionario de datos	H	9	86	95
J	2.1Análizar el desarrollo, tiempos de diseño de la aplicación	I	10	95	105
K	2.2 Realizar diseño externo del software	J	10	105	115
L	2.3 Realizar diseño de datos	K	7	115	122
M	2.4 Realizar diseño modular	L	7	115	122
N	2.5 Realizar diseño procedimental	M	7	115	122
O	3.1 Desarrollar Software	L,M,N	40	122	162
P	3.2 Ejecutar pruebas técnicas	O	15	162	177
Q	3.3 Entregar documento final del desarrollo	P	8	177	185
R	4.1 Verificar documento funcional final del desarrollo	Q	30	185	215
S	4.1.1 Realizar documento de casos de pruebas	R	10	215	225
T	4.2 Ejecutar Pruebas de compatibilidad	S	20	225	245
U	4.3 Ejecutar Pruebas de regresión	T	10	245	255
V	4.4 Ejecutar Pruebas de integración	U	20	245	265
W	5.1 Preparar y documentar la capacitación del software	T,U,V	8	265	273
Z	5.2 Realizar las capacitaciones	W	5	273	278
Y	5.3 Diligenciar registro de capacitaciones	Z	5	278	283
Z	5.4 Realizar manuales de operación y mantenimiento de software	Y	15	283	298
AA	5.5 Documentar el proceso del canal Banca móvil	Z	10	298	308
AB	6.1 Realizar la puesta en producción	AA	10	308	318
AC	7.1 Realizar documento de historia del proyecto. (DHP)	AB	8	318	326

Para la estimación de la duración de las actividades y del orden en que se deben ejecutar se utilizó información histórica de experiencias adquiridas en proyectos similares de implementación de sistemas de seguimiento y control para los fraudes transaccionales. Del cronograma se concluye que la implementación de un sistema de control de fraudes tendría una duración aproximada de 360 días. La mejor forma de ver el orden en que se desarrollan las actividades es mediante un diagrama de red, el cual podemos ver en la Ilustración 3, que se encuentra a continuación.

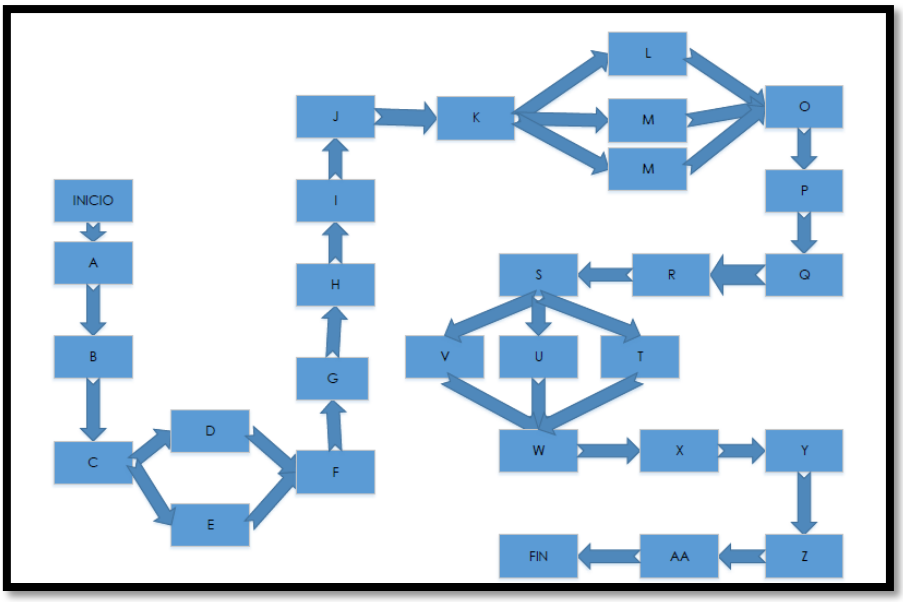

Ilustración 3: Diagrama de red.

2.4.4 Obtener la ruta critica

La ruta crítica es la secuencia de los elementos terminales de la red de proyectos con la mayor duración entre ellos, determinando el tiempo más corto en el que es posible completar el proyecto. En la ilustración 4, se presentara en color verde la ruta crítica donde se determinó la duración del proyecto entero. Cualquier retraso en un elemento de la ruta crítica afecta a la fecha de término planeada del proyecto, y se dice que no hay holgura en la ruta crítica.

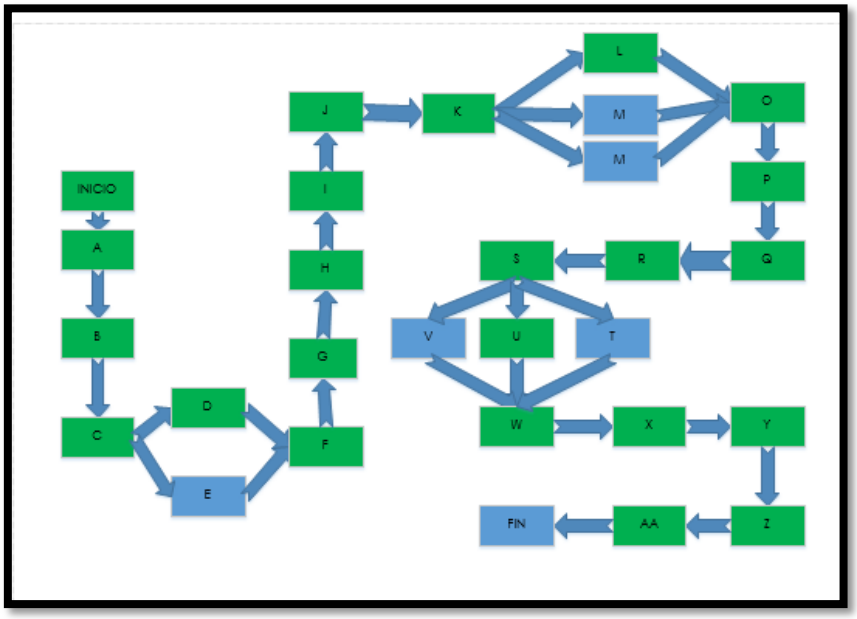

Ilustración 4: Estructura de desglose de trabajo EDT.

2.5 Gestionar los costos

Para la gestión de costos es necesario definir los costos de mano de obra y la estructura de costos, en los apartados 2.4.1 y 2.4.2, que se encuentran a continuación se detallara cada paso para la gestión de costos.

2.5.1 Mano de obra

La mano de obra se contrata de acuerdo al perfil relacionado en el numeral 2.2.1.4 Recursos, de acuerdo a la perfil y funciones que se requiriera para que el proyecto se ejecute en un año, en la tabla 6 se relacionan los costos de mano de obra los cuales tiene un valor de $150.949.179 pesos colombianos.

Tabla 6. Costos Mano de obra

Cargo	*valor mensual*	*VALOR TOTAL*
Gerente de Proyecto	$ 3.500.000	$ 42.000.000
Líder Técnico	$ 3.166.667	$ 38.000.000
Asesor funcional	$ 1.300.000	$ 18.437.728
Líder de Pruebas	$ 2.000.000	$ 8.495.919
Diseñador Grafico	$ 1.250.000	$ 3.234.396
Arquitecto de Software	$ 2.500.000	$ 25.000.000
Desarrollador Senior	$ 2.500.000	$ 25.000.000
		$ 160.168.043

2.5.2 Estructura de costos

Los costos de implementación dan un total de $ 180.168.043 de pesos colombianos, para un valor total del presupuesto con IVA de $ 208.994.930 de pesos colombianos, proyectado a 12 meses.

Tabla 7. Estructura de costos

Estructura de costos	VR. TOTAL (Miles $)
Total mano de obra	$ 160.168.043
Total Costos Indirectos	$ 5.000.000
Total Gastos de venta	$ 2.000.000
Total Gastos de Administración	$ 3.000.000
Total Gastos financieros	$ 5.000.000
Total Costos	$ 5.000.000
Total propuesta sin IVA	$ 180.168.043
IVA	$ 28.826.887
Total Propuesta	$ 208.994.930

3 CONCLUSIONES

- En el desarrollo de productos de software las etapas de análisis de requerimientos y diseño toma gran parte del tiempo del proyecto. El modelo planteado en este proyecto pretende establecer unos parámetros de diseño generales que permitan agilizar la implementación de proyectos tipo sistemas de control por software.
- Siguiendo las actividades sugeridas en el modelo V, se presentan beneficios al tener una estructura homogénea y clara reflejada en el diseño y la codificación del producto de software para el seguimiento y control de fraudes transaccionales.
- Implementar la estrategia en la planeación apoyando a cada uno de los grupos de trabajo como parte de la calidad en el proyecto fue fundamental para el desarrollo de software en un sistema TSP.
- Es muy importante efectuar el control exhaustivo en cada actividad y/o tarea asignada en cada etapa de desarrollo y diseño para garantizar el éxito del cronograma.

- El software deberá cumplir con detectar posibles riesgos de fraudes en medios de pagos con tarjeta débito.

- Aumentar la seguridad incrementando procesos de ingresos más seguros controlando cada transacción realizada por el cliente.

- Con el constante desarrollo e innovación de las tecnologías utilizadas en las implementaciones de software, se realizó un modelo funcional para el diseño del software para el seguimiento y control de fraudes transaccionales desde internet y banca móvil con tarjeta debito bajo los lineamientos del PMI.

- Presentar un cambio radical a los procesos actuales del ingreso a portal internet y banca móvil, con nuevas tecnologías tales como: bases de datos SQL, interfaz de usuario en plataforma Web. Y a través de la integración con sistemas en plataforma Windows y sistemas en plataforma IONES, WINDOWS PHONE Y ANDROID, permitiendo de ésta forma entregar un modelo alternativo a los procesos actuales de captación de clientes y entrega de tarjetas de débito.

REFERENCIAS BIBLIOGRAFICAS

[1] Superintendencia Financiera de Colombia. (25 de octubre de 2007). [Capítulo Décimo Segundo del Título I de la Circular Básica Jurídica – Circular Externa 007 de 1996]. Requerimientos mínimos de seguridad y calidad en el manejo de información a través de medios y canales de distribución de productos y servicios para clientes y usuarios. [Circular Externa 052 de 2007]. Recuperado de: https://www.superfinanciera.gov.co/jsp/loader.jsf?lServicio=Publicaciones&lTipo=publicaciones&lFuncion=loadContenidoPublicacion&id=20145.

[2] Finanzas personales (25 de octubre de 2010) Como suceden los fraudes electrónicos. Recuperado de:http://www.finanzaspersonales.com.co/gaste-eficientemente/articulo/como-suceden-los-fraudes-electronicos/37912.

[3]Mediante la Circular Externa 042 de 2012, la Superintendencia realizó algunas modificaciones al referido Capítulo Décimo Segundo del Título Primero de la Circular Básica Jurídica, relacionado con los requerimientos mínimos de seguridad y calidad para la realización de operaciones, en específico, adicionó los numerales 2.15, 2.16, 2.17, 2.18, 4.2.7, 4.6.3, 4.9.7, 4.9.8, 4.11 y 6.12; y modificó el contenido de los numerales 2.3, 2.4, 3.1.7, 3.2.2, 3.3.3, 3.3.10, 4.7.5, 6.10 y 6.11. Todas estas modificaciones posteriormente fueron incluidas en la Circular Externa 029 de 2014, la cual reexpidió la Circular Básica Jurídica de esta Superintendencia.

[4] Ibidem. Subnumeral 2.4 literal c) “Instrumentos para la realización de operaciones” [Capítulo XII del Título I de la Circular Básica Jurídica – Circular Externa 007 de 1996]. [Circular Externa 042 de 2012] Ibidem. Subnumeral 2.3.4.9 “Internet”.

[5] Ibidem. Subnumerales 2.3.5 y 2.3.7 “Requerimientos en materia de actualización de software” y “Análisis de vulnerabilidades”.